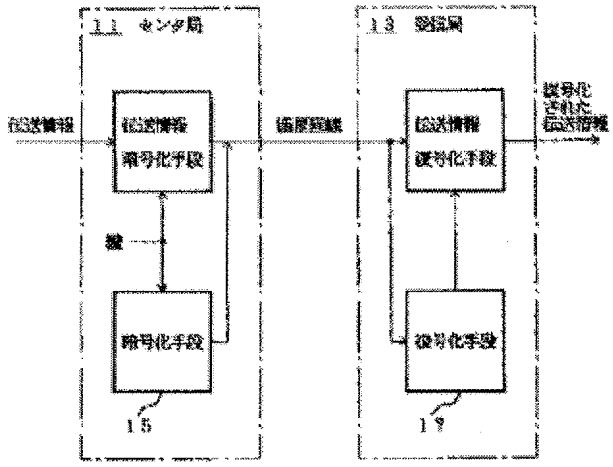
# CIPHERING TRANSMISSION SYSTEM

**Publication number:** JP5167575
**Publication date:** 1993-07-02
**Inventor:** TAMURA MASAHIRO
**Applicant:** FUJITSU LTD
**Classification:**
**- international:** ***H04K1/00; H04L9/06; H04L9/08; H04L9/14;*** **H04K1/00; H04L9/06; H04L9/08; H04L9/14;** (IPC1-7): H04K1/00; H04L9/06; H04L9/14
**- European:**
**Application number:** JP19910335026 19911218
**Priority number(s):** JP19910335026 19911218

Report a data error here

Abstract of **JP5167575**

PURPOSE:To improve the secrecy of transmission information in a satellite line, regarding a ciphering transmission system performing transmission and receptions by ciphering transmission information between mutual earth stations opposing via the satellite line, in a satellite communication system.
CONSTITUTION:In a ciphering transmission system provided with a center station 11 transmitting transmission information to a satellite line by ciphering it based on a prescribed key and a reception station 13 receiving the ciphered transmission information from the satellite line and decoding it, the center station 11 is provided with a ciphering means 15 ciphering the key and transmitting it to the satellite line. The reception station 13 is composed by being provided with a deciphering means 17 receiving the ciphered key from the satellite line and obtaining the key to make the deciphering processing of the transmission information efficient by performing a deciphering processing opposite to the ciphering processing to be performed by the ciphering means 15.




Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

**特開平5－167575**

(43)公開日　平成５年(1993)７月２日

| (51)Int.Cl.[5] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/06 | | | | | |
| | 9/14 | | | | | |
| Ｈ０４Ｋ | 1/00 | | Ｚ　7117－5Ｋ | | | |
| | | | 7117－5Ｋ | Ｈ０４Ｌ　9／02 | | Ｚ |

審査請求　未請求　請求項の数１(全　６　頁)

(21)出願番号　特願平3－335026

(22)出願日　平成３年(1991)12月18日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　田村　昌宏
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　古谷　史旺

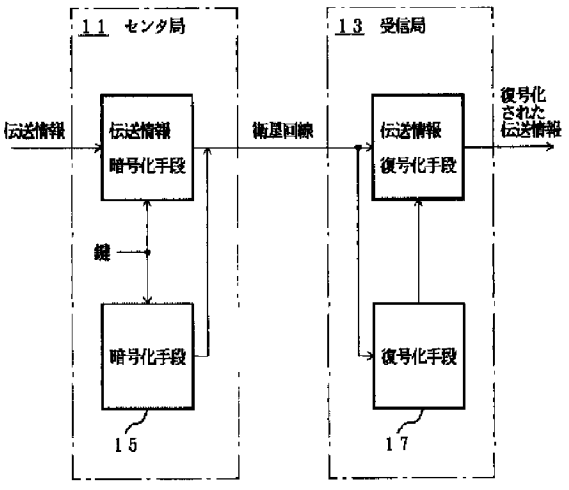
(54)【発明の名称】　暗号化伝送方式

(57)【要約】

【目的】　本発明は、衛星通信システムにおいて、衛星回線を介して対向する地球局相互間で伝送情報を暗号化して送受する暗号化伝送方式に関し、衛星回線における伝送情報の秘匿性を高めることができることを目的とする。

【構成】　伝送情報を所定の鍵に基づいて暗号化して衛星回線に送信するセンタ局１１と、衛星回線から暗号化された伝送情報を受信して復号化する受信局１３とを備えた暗号化伝送方式において、センタ局１１には、鍵を暗号化して衛星回線に送信する暗号化手段１５を備え、受信局１３には、衛星回線から暗号化された鍵を受信し、かつ暗号化手段１５が行う暗号化処理と反対の復号化処理を施して伝送情報の復号化処理を効率化する鍵を得る復号化手段１７を備えて構成される。

本発明の原理ブロック図



1

【特許請求の範囲】

【請求項1】　伝送情報を所定の鍵に基づいて暗号化して衛星回線に送信するセンタ局（１１）と、
前記衛星回線から前記暗号化された伝送情報を受信して復号化する受信局（１３）とを備えた暗号化伝送方式において、
前記センタ局（１１）には、前記鍵を暗号化して前記衛星回線に送信する暗号化手段（１５）を備え、
前記受信局（１３）には、前記衛星回線から前記暗号化された鍵を受信し、かつ前記暗号化手段（１５）が行う暗号化処理と反対の復号化処理を施して前記伝送情報の復号化処理を効率化する鍵を得る復号化手段（１７）を備えたことを特徴とする暗号化伝送方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、衛星通信システムにおいて、衛星回線を介して対向する地球局相互間で伝送情報を暗号化して送受する暗号化伝送方式に関する。

【０００２】

【従来の技術】衛星回線を介して企業内および企業間のメールの送受を行う衛星通信システムでは、例えば、新製品を開発中の研究所と関連部門との間で送受されたメールの内容が同一分野の競業他社に漏洩して莫大な損失を被ることを回避するために、そのメールに含まれる文書や画像情報を暗号化して衛星回線に送出する暗号化伝送方式が採用される。

【０００３】暗号化伝送方式としては、例えば、送信される伝送情報にM系列のＰＮ符号との乗算処理を施す簡単な処理によって伝送情報の秘匿性を得る方式が一般的であるが、このような方式の暗号化出力は、暗号化について初歩的な知識を有する者であれば容易に復号化可能であるために、伝送情報について得られる秘匿性は極めて低い。

【０００４】したがって、衛星通信システムでは、種々の暗号化方式の内、特に米国商務省標準局（ＮＢＳ）の公募に対してＩＢＭ社が提案したＤＥＳ（Data EncryptionStandard）方式が、暗号化方式を開示して復号化に必要な鍵を秘密とすることによって高い秘匿性が得られ、かつこのような特性から暗号・復号化装置やその装置に等価な処理を行うソフトウエアを容易に実現できるので、従来より採用されている。

【０００５】図４は、暗号化伝送方式を用いた衛星通信システムの構成例を示す図である。図において、センタ局４１と受信局４２とは衛星回線を介して対向配置され、センタ局４１では、伝送情報は暗号器４３を介して送信機４４の一方の入力に与えられ、その出力は衛星回線に接続される。サブネットワーク暗号鍵生成器４５の出力は、暗号器４３の鍵入力と送信器４４の他方の入力に与えられる。

【０００６】受信局４２では、衛星回線が受信機４６の

2

入力に接続され、その一方の出力は復号器４７の一方の入力に接続される。受信機４６の他方の出力は復号器４７の鍵入力に接続され、その出力には復号化された伝送情報が得られる。

【０００７】このような構成の衛星通信システムでは、センタ局４１の送信機４４は、伝送情報の送信に先行して、衛星回線にサブネットワーク暗号鍵生成機４５が出力する暗号鍵を暗号化せずに送信する。さらに、暗号器４３は、サブネットワーク暗号鍵生成器４５から与えられるサブネットワーク暗号鍵に基づいて上述したＤＥＳ方式による伝送情報の暗号化を行い、その暗号化出力を送信機４４を介して衛星回線に送出する。

【０００８】受信局４２では、受信機４６は、衛星回線を介してセンタ局４１から受信されたサブネットワーク暗号鍵を復号器４７の鍵入力に与え、さらに、その鍵に続いてセンタ局４１から受信された伝送情報を復号器４７に与える。復号器４７は、上述したサブネットワーク暗号鍵を用いてセンタ局４１から暗号化されて受信された伝送情報を復号化する。

【０００９】

【発明が解決しようとする課題】ところで、このような従来の暗号化伝送方式では、サブネットワーク暗号鍵が暗号化されずに衛星回線に送出されるために、第三者によって鍵の内容が知られて伝送情報が容易に復号化される可能性があった。

【００１０】本発明は、衛星回線における伝送情報の秘匿性を高めることができる暗号化伝送方式を提供することを目的とする。

【００１１】

【課題を解決するための手段】図１は、本発明の原理ブロック図である。本発明は、伝送情報を所定の鍵に基づいて暗号化して衛星回線に送信するセンタ局１１と、衛星回線から暗号化された伝送情報を受信して復号化する受信局１３とを備えた暗号化伝送方式において、センタ局１１には、鍵を暗号化して衛星回線に送信する暗号化手段１５を備え、受信局１３には、衛星回線から暗号化された鍵を受信し、かつ暗号化手段１５が行う暗号化処理と反対の復号化処理を施して伝送情報の復号化処理を効率化する鍵を得る復号化手段１７を備えたことを特徴とする。

【００１２】

【作用】本発明では、センタ局１１では伝送情報を暗号化する際に用いられる鍵が暗号化手段１５によって暗号化されて衛星回線に送信され、受信局１３では、復号化手段１７がこのようにしてセンタ局１１から衛星回線を介して送信された鍵を復号化して伝送情報の復号化を効率的に行うために必要な鍵を得る。

【００１３】すなわち、受信局１３は、センタ局１１から暗号化して送信された鍵に基づいて伝送情報を復号化するので、その鍵が衛星回線上で第三者に傍受されて

も、その第三者は、復号化手段１７が行う復号化処理のアルゴリズムやその処理に必要な鍵を知らないかぎり、容易に伝送情報を復号化することはできない。

【００１４】

【実施例】以下、図面に基づいて本発明の実施例について詳細に説明する。図２は、本発明の一実施例を示す図である。

【００１５】図において、図４に示すものと機能および構成が同じものについては、同じ参照番号を付与して示し、ここではその説明を省略する。本実施例と図４に示す従来例との相違点は、センタ局４１に代わるセンタ局２１では、サブネットワーク暗号鍵生成器４５と送信機４４の他方の入力との間にセット個別鍵に基づいてサブネットワーク暗号鍵を暗号化する暗号器２２を配置すると共に、受信局２５に付与すべきパスワードを鍵としてセット個別鍵を暗号化し、かつその暗号化出力をカード２３に記録するスクランブラ２４を備え、受信局４２に代わる受信局２５では、受信機４６の出力と復号器４７の鍵入力との間に復号器２６を配置し、かつ上述したパスワードとカード２３に記録された情報とに応じてセット個別鍵と同じ鍵を復号器２６の鍵入力に与えるデ・スクランブラ２７を備えた点にある。

【００１６】なお、本実施例と図１に示すブロック図との対応関係については、センタ局２１はセンタ局１１に対応し、受信局２５は受信局１３に対応し、暗号器２２、カード２３およびスクランブラ２４は暗号化手段１５に対応し、カード２３、復号器２６およびデ・スクランブラ２７は復号化手段１７に対応する。

【００１７】以下、図２を参照して本実施例の動作を説明する。センタ局２１では、受信局の管理を行うシステム管理者は、受信局２５が新たに開局するときにその受信局にパスワードを付与する。さらに、システム管理者は、そのパスワードを暗号化鍵とするＤＥＳ方式の暗号化処理をスクランブラ２４を介してセット個別鍵に施し、かつその暗号化出力をカード２３に書き込んで受信局２５に送付する。

【００１８】伝送情報の暗号化は従来例と同様にＤＥＳ方式のＯＦＢ(Output Feedback) モードによって行われるが、暗号器２２は、その伝送情報の送信に先行してサブネットワーク暗号鍵にセット個別鍵を鍵としたＤＥＳ方式のＥＣＢ(Electric CodeBook) モードによる暗号化処理を施す。送信機４１は、このようにして暗号化されたサブネットワーク暗号鍵を受信局２５に送信する。なお、このように暗号化されたサブネットワーク鍵および伝送情報は、衛星放送のデータチャネルフレームを介して送受され、図３に斜線で示すように、そのフレームの先頭に配置されたフレーム同期符号、フレーム制御符号、レンジ符号を除く後半部分に、ブロック長が６３ビットでパリティビット数が５６のプリミティブ多項式に基づくＢＣＨコードに符号化されて配置される。



【００１９】一方、受信局２５では、システム管理者から送付されたカード２３がデ・スクランブラ２７に装着され、デ・スクランブラ２７は、カード２３に書き込まれた情報と上述したパスワードとに基づいてセンタ局２１のスクランブラ２４と反対の処理を行ってセット個別鍵を生成する。復号器２６は、このようにして得られたセット個別鍵を鍵とする復号化処理をセンタ局２１から暗号化して受信されたサブネットワーク暗号鍵に施す。復号化されたサブネットワーク暗号鍵は復号器４７の鍵入力に与えられるので、復号器４７は従来例と同様にしてセンタ局２１から暗号化して送信された伝送情報を復号化できる。

【００２０】このように本実施例によれば、衛星回線を介して受信局に送信されるサブネットワーク鍵はセット個別鍵を用いて暗号化され、かつ受信局ではそのセット個別鍵を復号化して伝送情報の復号化処理を行うので、衛星回線を介して伝送されるサブネットワーク鍵が第三者によって傍受されても、その鍵の送信先である受信局にカードに記録されて送付された別の暗号鍵が無ければ伝送情報を容易に復号化することはできない。

【００２１】また、本実施例は、サブネットワーク暗号鍵および伝送情報の伝送フレームは、衛星放送のデータチャネルフレーム（音楽データ伝送フレーム）の基本構成を保持して形成できるので、既存のセンタ局および受信局の装置にサブネットワーク暗号鍵の暗号化・復号化手段を付加することによって容易に実現できる。

【００２２】さらに、サブネットワーク鍵はセンタ局と全ての受信局との間で並行して同じものが用いられるが、その内容については、実際の運用システムでは、例えば、一週間毎に更新することによって秘匿性が確保される。

【００２３】なお、本実施例では、伝送情報の暗号化方式としてＤＥＳ方式を採用したが、本発明は、このような暗号化方式に限定されず、システムに要求される伝送効率や秘匿性が確保できるならば、どのような暗号化方式を用いてもよい。

【００２４】また、本実施例では、サブネットワーク暗号鍵もＤＥＳ方式に基づいて暗号化されるが、本発明は、このような暗号化方式に限定されず、例えば、公開鍵方式や鍵事前配布方式の暗号化方式を用いてもよい。

【００２５】さらに、本実施例では、放送衛星のデータチャネルを用いたデータ通信システムの一例を示したが、本発明は、このような通信システムに限定されず、対向する地球局間で衛星回線を介して伝送情報を暗号化して送受するシステムであれば、どのような衛星通信システムにも適用可能である。

【００２６】また、本実施例では、受信局に対するセット個別鍵の配送時の秘匿性を確保するために、パスワードを鍵とするセット個別鍵の暗号化処理の出力をカードに記録して受信局に送付しているが、本発明は、このよ

5

うなセット個別鍵の配送方式の如何にかかわらず適用できる。

【００２７】

【発明の効果】以上説明したように本発明は、センタ局は伝送情報の暗号化に用いる鍵を暗号化して衛星回線に送信し、受信局はこのようにして送信された鍵を復号化して伝送情報の復号化に用いるので、万一、衛星回線上で第三者に鍵が傍受されても、その鍵の復号化処理のアルゴリズムやその処理に必要な鍵が知られない限り、伝送情報が第三者に容易に漏洩することはない。

【００２８】したがって、衛星回線上おける伝送情報の秘匿性が向上し、衛星回線を利用したデータ通信の安全性が高められる。

【図面の簡単な説明】

【図１】本発明の原理ブロック図である。

【図２】本発明の一実施例を示す図である。

【図３】衛星回線の伝送フレームの構成を示す図である。

6

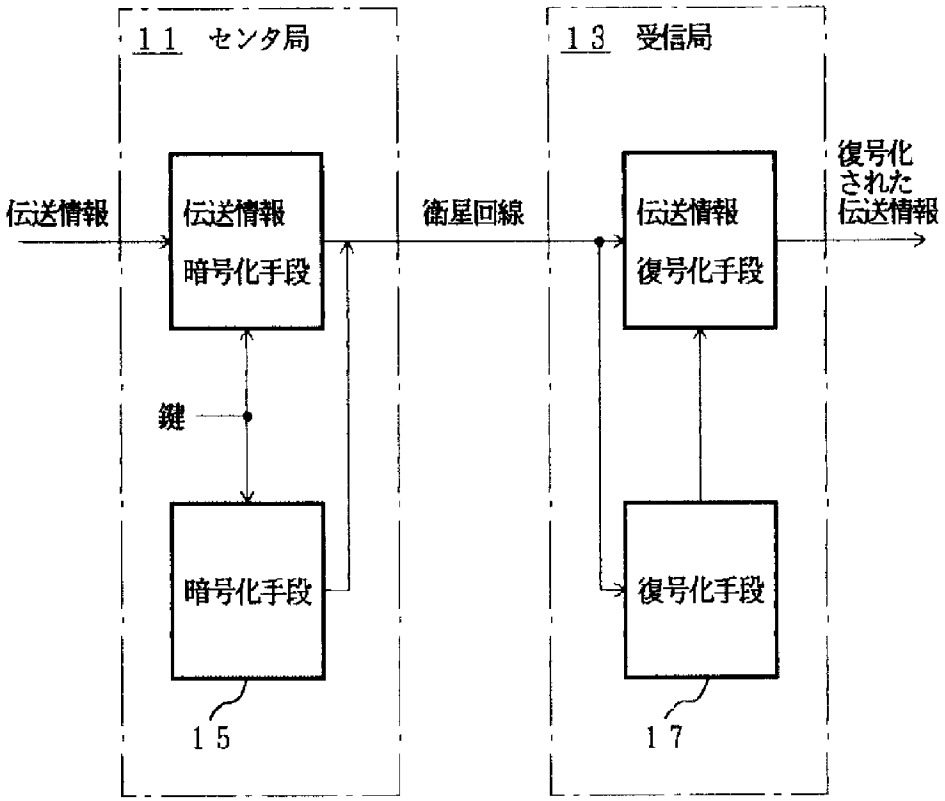
【図４】暗号化伝送方式を採用した衛星通信システムの構成例を示す図である。

【符号の説明】

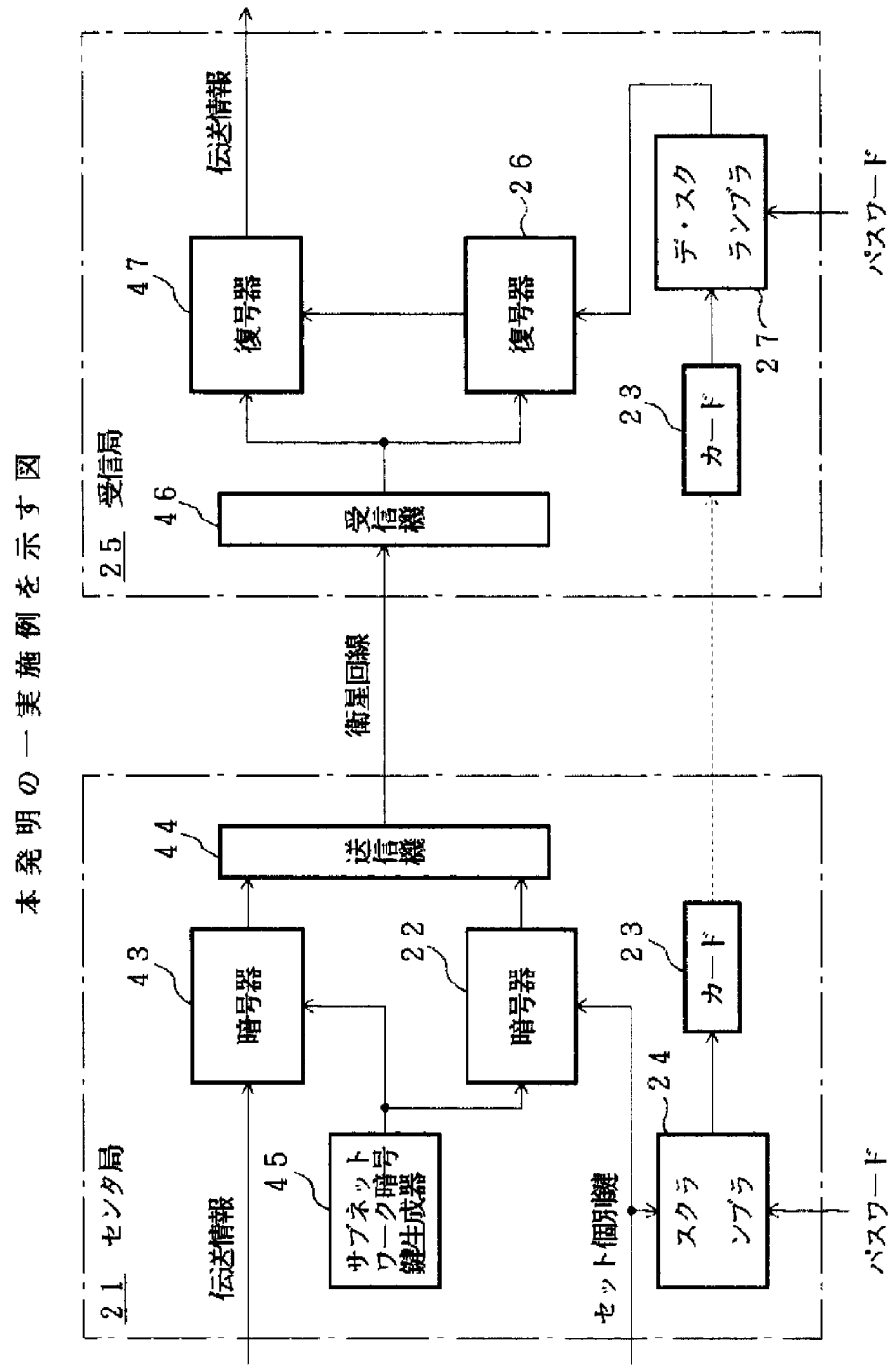
１１，２１，４１　センタ局
１３，２５，４２　受信局
１５　暗号化手段
１７　復号化手段
２２，４３　暗号器
２３　カード
２４　スクランブラ
２６，４７　復号器
２７　デ・スクランブラ
４４　送信機
４５　サブネットワーク暗号鍵生成器
４６　受信機

【図１】

本発明の原理ブロック図

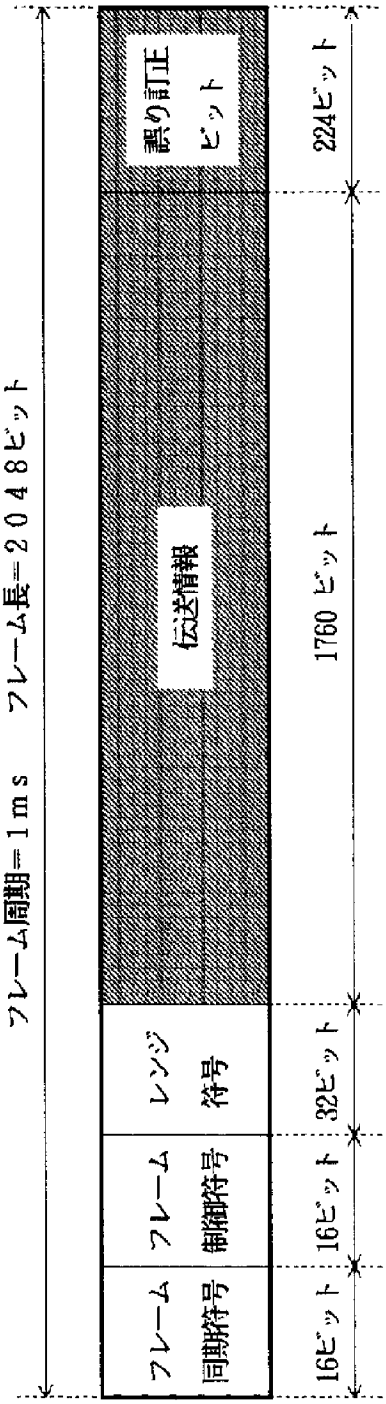


【図2】


本発明の一実施例を示す図
21 センタ局
25 受信局
伝送情報
衛星回線
送信機
受信機
暗号器
復号器
サブネットワーク暗号鍵生成器
カード
スクランブラ
デ・スクランブラ
パスワード
セット個別鍵
43
44
45
46
47
22
23
24
26
27

【図3】

衛星回線の伝送フレームの構成を示す図




【図4】

暗号化伝送方式を用いた衛星通信システムの構成例を示す図